

White Paper Project Proposal:

"The Personal Privacy Landscape: A Survey of the Relationship between Personal Privacy, Technology, and Policy"

Team and Participation in Group

Parvez Anandam

- Writing Chapter 2
- Writing Conclusions

Jessica Miller

- Organizing outline/proposal
- Writing Introduction
- Writing Chapter 3

Santeri Voutilainen

- Organizing outline
- Writing Chapter 4
- Writing Conclusions

Vitaliy Zavesov

- Organizing outline
- Writing Chapter 2
- Writing Conclusions

Paper Summary

In this paper, we will survey the current relationship between personal privacy and technology. We will begin by investigating why personal privacy is such a concern today. Particularly, we will investigate how the state-of the art in technology has evolved and what the impact on privacy attitudes have been. Next, in Chapter 2, we will explore the human organizations that want to collect/analyze personal information, the technologies they are using (or will use) that collect, analyze and store personal information, and the benefit/cost to the public of giving up their personal privacy to these organizations. Next, in Chapter 3, we will explore governmental and corporate policies (or lack thereof) that have been developed to protect privacy. We will look at laws in both the United States as well as internationally. We will also try to look for measures of success in these policies. Since personal privacy is such a concern, much research is being done in the technological domain about how to provide awareness without forsaking personal privacy. In Chapter 4, we will investigate current research that exposes data while maintaining privacy. This chapter will conclude with policy recommendations, with justifications, on why or why not these current methods are sufficient to adequately protect privacy while providing access to the data. Our last chapter concludes by summarizing what we have learned and where we would like to see both technology and policy go from here.

Chapter 1: Introduction (i.e. why is personal privacy such a hot topic today?)

- 1) Why is personal privacy of such great concern today?
 - a. What we (as a group) mean by personal privacy
 - b. What we (as a group) are considering to be personal information
- 2) State-of-the-art in information capture and storage from past → present → future and how, with these changes, concern of privacy has escalated:

- a. Paper both capture and store information
- b. Mainframes
- c. Personal computers and Internet
- d. Ubiquitous computing
 - i. RFID
 - ii. Cell phones

Chapter 2: Organizational Threats to Personal Privacy and Technologies Used to Exploit Privacy (i.e. who would want my personal data, why and how are they accessing my data?)

- 1) National security agencies (security and privacy are frequently at odds)
 - a. Especially a hot topic now with worries of terrorism
 - b. RFID in passports example
 - c. Other surveillance mechanisms
 - d. Cost to “users” – privacy
 - e. Benefit to “users” – security (?)
- 2) Advertising agencies – commercial purposes
 - a. Use of Internet to get personal data for advertising purposes
 - i. Adware
 - ii. Spyware
 - iii. Spam
 - b. Cost to “users”
 - c. Benefit to “users”
- 3) Insurance companies
 - a. Privacy about personal health information and HIPAA
- 4) Private companies – outside of advertisement reasons
 - a. Tracking employees
 - i. Keystroke logging
 - b. Tracking of equipment through RFID
 - i. Benefits
 1. Tracking of equipment and goods
 - ii. Cost
 1. Walmart/Benetton consumer backlash

Chapter 3: Current Policy to Protect Privacy

- 1) Privacy protection through policy in the U.S.
 - a. Privacy not a constitutional right
 - i. Implications of this
 - ii. Free speech in opposition privacy?
 - b. Laws protecting privacy
 - i. Wiretapping laws
 - ii. HIPAA
 - iii. Benefits/costs of such laws
 - c. Laws that infringe on personal privacy
 - i. Patriot Act
 - ii. Benefits/costs of such laws
- 2) International privacy protection through policy
 - a. EU Data Privacy Protection Act
 - i. How does this play out with American companies collecting information about Europeans on the Internet?
 - b. Other international initiative to protect personal data
 - i. I think Australia also has some laws in place...

- 3) Corporate privacy protection through policy
 - a. Privacy policies
 - i. Why they don't work
 - ii. Are these mandated or just good practice
 - b. Employee monitoring (employee rights)
- 4) Our recommendations/reflections on policy to protect personal data
 - a. Benefits vs. costs of protection with policy
 - b. Benefits vs. costs of no policy protection
 - c. Public's role in protecting their data
 - d. Relationship between government mandates and good business practice

Chapter 4: State-of-the-Art Technological Solutions that Expose Data While Protecting Privacy

- 1) general overview of the benefits of publicly available data, privacy, as well as an intro to the idea of combining both
- 2) methods that can be used to expose data while providing privacy
 - a. aggregate data
 - b. anonymization through exclusion, generalization and renaming
 - c. examples (commercial and academic) of each method
- 3) benefits and pitfalls of each method with respect to data access and personal privacy
- 4) Policy recommendations, with justifications, on why or why not these methods are sufficient to adequately protect privacy while providing access to the data

Chapter 5: Conclusion

Possible Sources

Articles on academic and commercial products, such as:

<http://www.msnbc.msn.com/id/4486823/site/newsweek/>

Controlling Access to Published Data Using Cryptography. Gerome Miklau and Dan Suciu. VLDB 2003, Proceedings of 29th International Conference on Very Large Data Bases, September 9-12, 2003, Berlin, Germany.

European Commission (2000). Proposal for a directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Retrieved November 11, 2005 at
<http://europa.eu.int/comm/information_society/policy/framework/pdf/com2000385_en.pdf>.

CMU Data Privacy Lab publications. <http://privacy.cs.cmu.edu/>

Electronic Privacy Information Center. <http://www.epic.org/>

Federal Trade Commission Privacy Initiatives. <http://www.ftc.gov/privacy/>

k-Anonymity: A Model For Protecting Privacy. Latanya Sweeney.
<http://privacy.cs.cmu.edu/people/sweeney/kanonymity.pdf>

Nabil R. Adam, John C. Wortmann: Security-Control Methods for Statistical Databases: A Comparative Study. ACM Computing Surveys 21(4): 515-556 (1989). Surveys methods for protecting statistical databases against disclosure of confidential information.